Splunk

Exam Questions SPLK-2002

Splunk Enterprise Certified Architect

NEW QUESTION 1
What does the deployer do in a Search Head Cluster (SHC)? (Select all that apply.)

A. Distributes apps to SHC members.
B. Bootstraps a clean Splunk install for a SHC.
C. Distributes non-search related and manual configuration file changes.
D. Distributes runtime knowledge object changes made by users across the SHC.

Answer: A

NEW QUESTION 2
Which of the following are client filters available in serverclass.conf? (Select all that apply.)

A. DNS name.
B. IP address.
C. Splunk server role.
D. Platform (machine type).

Answer: AB

NEW QUESTION 3
Which Splunk server role regulates the functioning of
indexer cluster?

A. Indexer
B. Deployer
C. Master Node
D. Monitoring Console

Answer: C

NEW QUESTION 4
When adding or rejoining a member to a search head cluster, the following error is displayed:
Error pulling configurations from the search head cluster captain; consider performing a destructive configuration resync on this search head cluster member.
What corrective action should be taken?

A. Restart the search head.
B. Run the splunk apply shcluster-bundle command from the deployer.
C. Run the clean raft command on all members of the search head cluster.
D. Run the splunk resync shcluster-replicated-config command on this member.

Answer: B

NEW QUESTION 5
A three-node search head cluster is skipping a large number of searches across time. What should be done to increase scheduled search capacity on the search head cluster?

A. Create a job server on the cluster.
B. Add another search head to the cluster.
C. server.conf captain_is_adhoc_searchhead = true.
D. Change limits.conf value for max_searches_per_cpu to a higher value.

Answer: D

NEW QUESTION 6
To activate replication for an index in an indexer cluster, what attribute must be configured in indexes.conf on all peer nodes?

A. repFactor = 0
B. replicate = 0
C. repFactor = auto
D. replicate = auto

Answer: C

NEW QUESTION 7
Splunk Enterprise platform instrumentation refers to data that the Splunk Enterprise deployment logs in the _introspection index. Which of the following logs are included in this index? (Select all that apply.)

A. audit.log
B. metrics.log
C. disk_objects.log
D. resource_usage.log

Answer: CD

NEW QUESTION 8
Which of the following can a Splunk diag contain?

A. Search history, Splunk users and their roles, running processes, indexed data
B. Server specs, current open connections, internal Splunk log files, index listings
C. KV store listings, internal Splunk log files, search peer bundles listings, indexed data
D. Splunk platform configuration details, Splunk users and their roles, current open connections, index listings

Answer: B

NEW QUESTION 9
At which default interval does metrics.log generate a periodic report regarding license utilization?

A. 10 seconds
B. 30 seconds
C. 60 seconds
D. 300 seconds

Answer: B

NEW QUESTION 10
Which of the following statements describe a Search Head Cluster (SHC) captain? (Select all that apply.)

A. Is the job scheduler for the entire SHC.
B. Manages alert action suppressions (throttling).
C. Synchronizes the member list with the KV store primary.
D. Replicates the SHC's knowledge bundle to the search peers.

Answer: AD

NEW QUESTION 10
Which command is used for thawing the archive bucket?

A. Splunk collect
B. Splunk convert
C. Splunk rebuild
D. Splunk dbinspect

Answer: C

NEW QUESTION 15
In which phase of the Splunk Enterprise data pipeline are indexed extraction configurations processed?

A. Input
B. Search
C. Parsing
D. Indexing

Answer: C

NEW QUESTION 16
When troubleshooting monitor inputs, which command checks the status of the tailed files?

A. splunk cmd btool inputs list | tail
B. splunk cmd btool check inputs layer
C. curl https://serverhost:8089/services/admin/inputstatus/TailingProcessor:FileStatus
D. curl https://serverhost:8089/services/admin/inputstatus/TailingProcessor:Tailstatus

Answer: C

NEW QUESTION 18
Of the following types of files within an index bucket, which file type may consume the most disk?

A. Rawdata
B. Bloom filter
C. Metadata (.data)
D. Inverted index (.tsidx)

Answer: B

NEW QUESTION 21
Which of the following should be done when installing Enterprise Security on a Search Head Cluster? (Select all that apply.)

A. Install Enterprise Security on the deployer.

B. Install Enterprise Security on a staging instance.
C. Copy the Enterprise Security configurations to the deployer.
D. Use the deployer to deploy Enterprise Security to the cluster members.

Answer: AD

NEW QUESTION 26
As a best practice, where should the internal licensing logs be stored?

A. Indexing layer.
B. License server.
C. Deployment layer.
D. Search head layer.

Answer: D

NEW QUESTION 30
When Splunk is installed, where are the internal indexes
stored by default?

A. SPLUNK_HOME/bin
B. SPLUNK_HOME/var/lib
C. SPLUNK_HOME/var/run
D. SPLUNK_HOME/etc/system/default

Answer: B

NEW QUESTION 33
Which of the following tasks should the architect perform when building a deployment plan? (Select all that apply.)

A. Use case checklist.
B. Install Splunk apps.
C. Inventory data sources.
D. Review network topology.

Answer: D

NEW QUESTION 37
Because Splunk indexing is read/write intensive, it is important to select the appropriate disk storage solution for each deployment. Which of the following statements is accurate about disk storage?

A. High performance SAN should never be used.
B. Enable NFS for storing hot and warm buckets.
C. The recommended RAID setup is RAID 10 (1 + 0).
D. Virtualized environments are usually preferred over bare metal for Splunk indexers.

Answer: C

NEW QUESTION 42
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SPLK-2002 Practice Exam Features:

* SPLK-2002 Questions and Answers Updated Frequently

* SPLK-2002 Practice Questions Verified by Expert Senior Certified Staff

* SPLK-2002 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SPLK-2002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year